



# Hardening Joomla! (MNI)

Web Security SS10

Leitung: Prof. Dr. Klaus Quibeldey-Cirkel

# Inhalt

- \* Einführung
- \* Giessen Aegis
- \* Suhosin
- \* Sicherheitstests: OWASP-Top Ten Risks
- \* Livedemo
- \* Fazit

# Einführung

- \* Ziel des Projektes: Implementierung einer Sicherheitsarchitektur für Joomla! (1.5)
- \* Voraussetzungen:
  - \* Integration von PHPIDS
  - \* Implementierung eines IPS
  - \* Statistische Auswertung
  - \* Tests mit JMeter
  - \* Integration von Suhosin
  - \* Sicherheitstests basierend auf den OWASP Top 10 Risks

# Giessen Aegis

- \* Plugin plg\_giessenAegis
- \* ReCaptcha
- \* Komponente com\_giessenAegis
- \* Modul mod\_giessenAegis
- \* Tests mit Jmeter
- \* Weiteres Backendmodul mod\_phpConfigCheck

# Plugin plg\_giessenAegis

- \* PHPIDS berechnet aufgrund Benutzeraktivitäten eine numerische Bedrohungsschwelle
- \* Diese Schwelle (Threshold) wird für die Ausführung d. Schutzmaßnahmen genutzt.
- \* Die Palette der Schutzmaßnahmen beinhaltet:
  - \* Logging
  - \* E-Mail Benachrichtigung
  - \* Warnung an den Benutzer
  - \* Ausloggen der Benutzer
  - \* Bannung der Benutzerkonto oder Benutzer IP

# Plugin plg\_giessenAegis

- \* Log Dateien und E-Mail Nachrichten enthalten:
  - \* Benutzer ID/IP
  - \* Datum
  - \* URL der Quellseite
  - \* Impact (PHPIDS-Bedrohungsschwelle)
  - \* Benutzereingabe
  - \* Benutzte Methode (GET/POST/...)
  - \* Enthaltende Angriffsarten (xss/csrf/id/...)
  - \* Beschreibung der Angriff in Wörter

# Plugin plg\_giessenAegis

- \* ... verfügt über weitere Funktionalität:
  - \* Falls die Komponente(com\_giessenaegis) installiert ist, werden die Angaben zu den Angriffen zusätzlich zur Log-Datei in der Datenbanktabelle gespeichert
  - \* White Lists: sowohl für den öffentlichen Bereich der Seite als auch für den Administrator
  - \* Bereiche können ausgewählte Ansichten als "Vertrauenswürdig" kennzeichnen und Eingaben in diesen Ansichten werden nicht vom Plugin ausgewertet

# Plugin plg\_giessenAegis

- \* ... verfügt über weitere Funktionalität:
  - \* Update der Filterlisten von PHPIDS auf Knopfdruck
  - \* Simulationsmodus ein-/ausschalten (IPS deaktivieren)
  - \* Anzeige der Logdatei
  - \* Löschen der Logdatei und Datenbankeinträge auf Knopfdruck
  - \* Einstellbarer Warning-Type (URL-Angabe bei Umleitung auf neue Seite)



# Plugin plg\_giessenAegis

## Backend:

The screenshot shows the Joomla! Backend interface for editing the 'plg\_giessenAegis' plugin. The top navigation bar includes 'Site', 'Menu', 'Content', 'Components', 'Extensions', 'Tools', and 'Help'. The main content area is titled 'Plugin: [Edit]' and contains two main sections: 'Details' and 'Parameters'.

**Details:**

- Name: giessenAegis
- Enabled: ☐ No ☒ Yes
- Type: system
- Plugin File: giessenAegis.php
- Access Level: Public (selected), Registered, Special
- Order: 0 (giessenAegis)
- Description: Integriert die PHPIDS (<http://php-ids.org/>) engine in ihre Joomla!-Installation

**Parameters:**

- Plugin Parameters:**
  - Log Threshold: 3
  - Mail Threshold: 10
  - Attack Mail Recipients: Markus Baier, Mark Othoff, Dennis Priefer, James Antrim, Björn Paar
  - Display Threshold: 25
  - Logout Threshold: 50
  - Ban Threshold: 100
  - Activity Time: 5
  - Giessen Aegis Component -Status: (Error icon)
- Advanced Parameters:**
  - Component Whitelist (frontend): com\_weblinks->iWeb Link, com\_weblinks->iWeb Link, com\_weblinks->iWeb Link, com\_weblinks->iWeb Link
  - Component Whitelist (backend): com\_weblinks->iWebLink, com\_weblinks->iWebLink, com\_pos->Pols, com\_pos->Pols

# ReCaptcha

- \* Gegenmaßnahme: **reCaptcha**
  - \* zum Schutz vor Crawlern und automatisierten Angriffen
  - \* Captcha bei zu vielen Requests in zu kurzer Zeit
    - \* zB: mittlere Zeit zwischen Requests bei 10 Requests insgesamt  $< 3$  Sekunden
  - \* Lösen des Captchas wird erzwungen
  - \* Umsetzung mit Komponenten aus dem Zend Framework

# ReCaptcha

## Anzeige des reCaptchas

Name  Passwort  Angemeldet bleiben ☐ Login   1 (0) Suchen

**MNI**  
FH GIESSEN-FRIEDBERG

Startseite Studium Forschung & Weiterbildung Fachbereich Lernplattform

QuickLinks

rise

sinkers

Type the two words:

  
stop spam.  
read books.

# Komponente com\_giessenAegis

- \* Dient der Statistischen Auswertung
- \* Beinhaltet zwei Datenbanktabellen
  - \* Sicherung der geloggten Angriffe
  - \* Auflistung der möglichen Attackentypen
- \* 3 Ansichten im Backend für den Administrator
  - \* Statistiken
  - \* Verwaltung
  - \* Attackentypen

# Komponente com\_giessenAegis

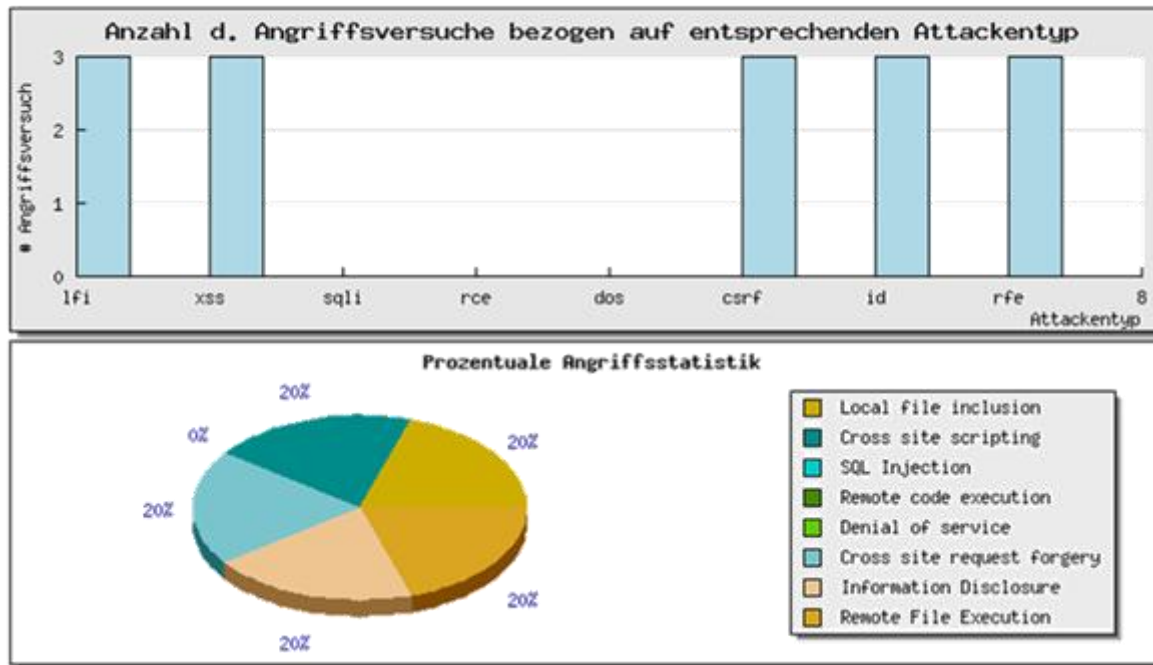
- \* Ansicht **Statistiken**:

- \* Unterschiedliche Statistiken zu geloggten Angriffen
  - \* Menge der verschiedenen Attacken
  - \* Prozentualer Anteil der verschiedenen Attackentypen
  - \* Auf Angreifer bezogene Statistiken
- \* Statistiken werden mit [JPGraph](#) dynamisch erstellt und angezeigt
- \* Einzeln abschaltbar
- \* Zeitspanne für die Anzeige kann angegeben werden

# Komponente com\_giessenAegis

## Backend:

Angezeigter Zeitraum: 06.09.2010 - 23.11.2010



# Komponente com\_giessenAegis

Backend:

**Giessen Aegis** [Speichern] [Abbrechen]

**Konfiguration**

	Anzahl der Angriffe bezogen auf entsprechende Attackentypen
Graph anzeigen	<input checked="" type="radio"/> Ja <input type="radio"/> Nein
Zeitraum (Beginn)	2010-09-06
Zeitraum (Ende)	2010-11-23

	Prozentuale Angriffsstatistik
Graph anzeigen	<input checked="" type="radio"/> Ja <input type="radio"/> Nein

	Anteil externer/interner Angriffsversuche
Graph anzeigen	<input checked="" type="radio"/> Ja <input type="radio"/> Nein
Zeitraum (Beginn)	2010-06-09
Zeitraum (Ende)	2020-06-01

	Anzahl der Angriffsversuche bezogen auf entsprechende Hosts
--	---

# Komponente com\_giessenAegis

- \* Ansicht **Verwaltung**:
  - \* Soll der Verwaltung der Statistiken dienen
  - \* Zeigt momentan nur gebannte User an
  - \* Gebannte User können in dieser Ansicht wieder freigegeben werden



# Komponente com\_giessenAegis

Backend:

Joomla! Fachbereich MNI Version 1.5.15

Site Menüs Inhalt Komponenten Erweiterungen Werkzeuge Hilfe

Vorschau 0 1 Abmelden

**Giessen Aegis**

Statistiken Verwaltung Attackentypen

Gebannte User:

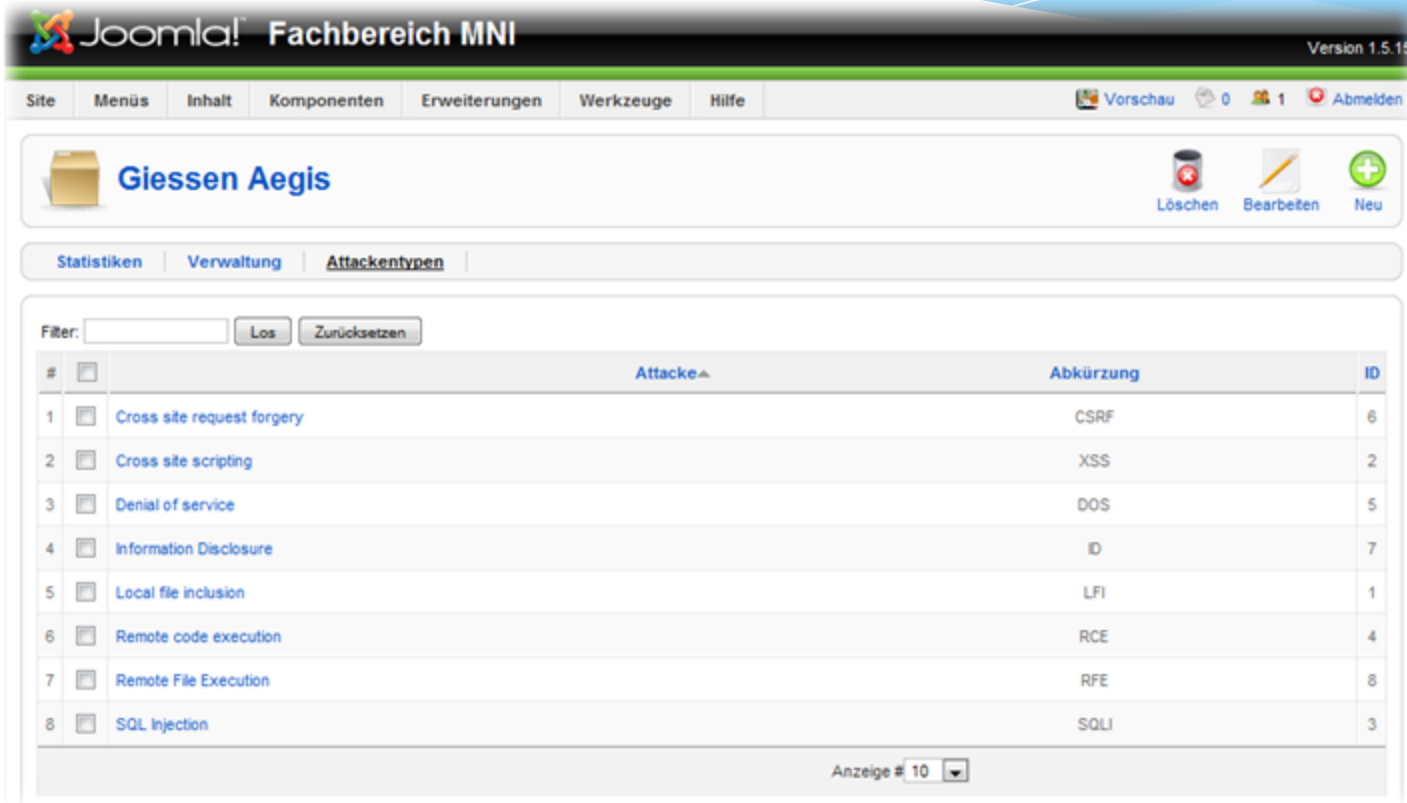
#		Benutzer
1		kneisel

# Komponente com\_giessenAegis

- \* Ansicht **Attackentypen**:
  - \* Zeigt eine Liste der eingetragenen Attackentypen
  - \* Eine nach PHPIDS gängige Liste ist bereits vordefiniert und in der Datenbank vorhanden
  - \* Man kann Attackentypen
    - \* neu eintragen
    - \* bearbeiten
    - \* Löschen
  - \* Dient nur der Zuordnung Langname  $\leftrightarrow$  Abkürzung

# Komponente com\_giessenAegis

## Backend:



Joomla! Fachbereich MNI Version 1.5.15

Site Menüs Inhalt Komponenten Erweiterungen Werkzeuge Hilfe

Vorschau 0 1 Abmelden

**Giessen Aegis** Löschen Bearbeiten Neu

Statistiken Verwaltung Attackentypen

Filter:  Los Zurücksetzen

#	<input type="checkbox"/>	Attacke▲	Abkürzung	ID
1	<input type="checkbox"/>	Cross site request forgery	CSRF	6
2	<input type="checkbox"/>	Cross site scripting	XSS	2
3	<input type="checkbox"/>	Denial of service	DOS	5
4	<input type="checkbox"/>	Information Disclosure	ID	7
5	<input type="checkbox"/>	Local file inclusion	LFI	1
6	<input type="checkbox"/>	Remote code execution	RCE	4
7	<input type="checkbox"/>	Remote File Execution	RFE	8
8	<input type="checkbox"/>	SQL Injection	SQLI	3

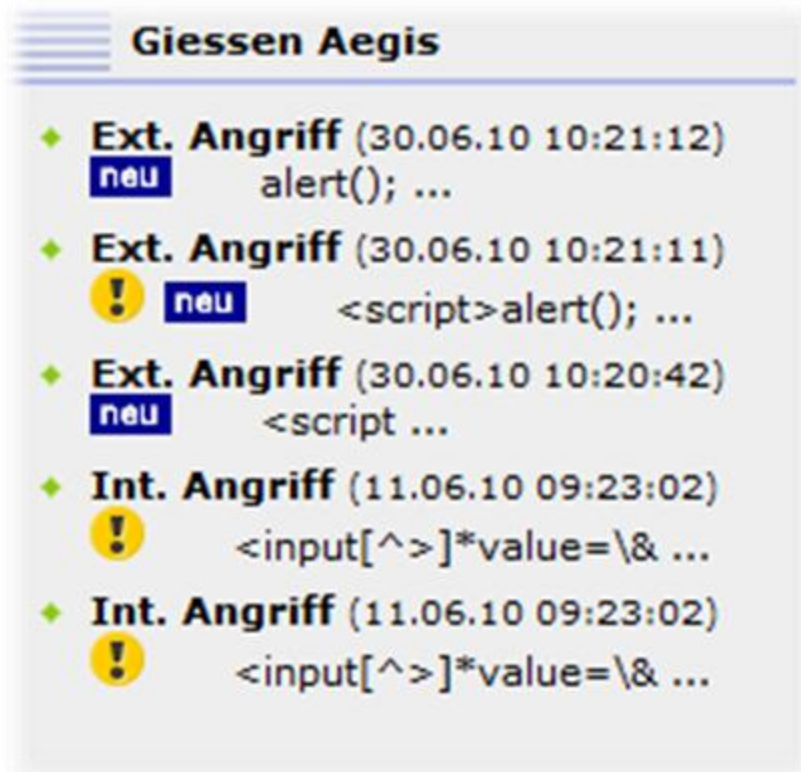
Anzeige # 10 ▼

# Modul mod\_giessenAegis

- \* Das Modul dient nur der Darstellung im Frontend
- \* Zeigt kompakt die letzten durchgeführten Attacken
- \* Detaillierte Infos können über Tooltips angezeigt werden
- \* Anzeige von Symbolen:
  - \* Neue Angriffe → „neu“-Symbol
  - \* Schwerwiegende Angriffe → Warnungssymbol
- \* Parametrisierbar im Backend

# Modul mod\_giessenAegis

## Frontend:



# Modul mod\_giessenAegis

## Frontend:

**Giessen Aegis**

- Ext. Angriff (30.06.10 10:21:12) **neu** alert(); ...
- Ext. Angriff (30.06.10 10:21:11) **!** **neu** <script>alert(); ...
- Ext. Angriff (30.06.10 10:21:11) **!** **neu** **Details**  
Angriffe: xss, csrf, id, rfe, lfi  
Impact: 16
- Int. Angriff (11.06.10 09:23:02) **!** <input[^>]\*value=\& ...
- Int. Angriff (11.06.10 09:23:02) **!** <input[^>]\*value=\& ...

**Giessen Aegis**

- Ext. Angriff (30.06.10 10:21:12) **neu** alert(); ...
- Ext. Angriff (30.06.10 10:21:11) **!** **neu** <script>alert(); ...
- Ext. Angriff (30.06.10 10:21:11) **!** **neu** **IP: 127.0.0.1**  
30.06.10 10:21:11 <script> ...
- Int. Angriff (11.06.10 09:23:02) **!** <input[^>]\*value=\& ...
- Int. Angriff (11.06.10 09:23:02) **!** <input[^>]\*value=\& ...

**Giessen Aegis**

- Ext. Angriff (30.06.10 10:21:12) **neu** alert(); ...
- Ext. Angriff (30.06.10 10:21:11) **!** **neu** <script>alert(); ...
- Ext. Angriff (30.06.10 10:21:11) **!** **neu** <script>alert();
- Int. Angriff (11.06.10 09:23:02) **!** <input[^>]\*value=\& ...
- Int. Angriff (11.06.10 09:23:02) **!** <input[^>]\*value=\& ...

# Modul mod\_giessenAegis

## Backend:

**Parameter**

▼ **Modulparameter**

Anz.d.Attacken	<input type="text" value="5"/>
Zeichenbeschr.	<input type="text" value="25"/>
Vektor anz.	<input checked="" type="radio"/> Aktivieren <input type="radio"/> Deaktivieren
Datum anz.	<input checked="" type="radio"/> Aktivieren <input type="radio"/> Deaktivieren
New-Icon anz.	<input checked="" type="radio"/> Aktivieren <input type="radio"/> Deaktivieren
Neu ab	<input type="text" value="5"/>
New-Icon	<input type="text" value="neu_blue_12.png"/> ▼
Warning-Icon anz.	<input checked="" type="radio"/> Aktivieren <input type="radio"/> Deaktivieren
Warning ab	<input type="text" value="10"/>
Warning-Icon	<input type="text" value="warning_1.png"/> ▼

# JMeter-Tests

- \* Externe Angriffe
  - \* SQL-Injections
  - \* XSS
- \* Interne Angriffe
  - \* Nach Login
  - \* SQL-Injections
  - \* XSS
  - \* Mehrfaches Absetzen der Angriffsvektoren um LogOut/Bannung zu simulieren



# Backendmodul mod\_phpConfigCheck

- \* Anzeige der php.ini-Einstellungen
- \* Vergleich mit empfohlenen Sicherheitseinstellungen

► Update nötig?		
► Suhosin		
▼ phpConfigCheck		
Config Option	Current Value	Recommended Value
register_globals	off	off
save_mode	off	on
open_base_dir	off	on
display_errors	1	off
allow_url_fopen	1	off
allow_url_include	off	off

# Suhosin

- \* Einbindung
- \* Konfiguration
- \* Backendmodul `mod_suhosin`

# Suhosin-Einbindung

- \* Server werden gegen bekannte und unbekannte Angriffsvektoren abgehärtet
- \* ausschließlich auf Linux Betriebssystemen verwendbar
- \* PHP Update auf Version 5.3.3
- \* Installation der Suhosin-Extension, sowie des Patches

# Suhosin-Konfiguration

- \* Angepasste Standard-Konfiguration
  - \* Anpassung erfolgte durch Studieren des Logfiles nach Antastverfahren auf dem Produktivsystem (Testsystem)
- \* Verknüpfung mit ClamAV
  - \* Neues Script zur Verknüpfung von ClamAV und Suhosin
  - \* Überprüfung von Dateien vor Upload

# Suhosin - Backendmodul

- \* Backendmodul mod\_suhosin:
  - \* Administration von Suhosin im Joomla!-Backend
  - \* Überprüfung und Anzeige, ob Suhosin-Installation verfügbar und aktuell
  - \* Schalter für An-/Abschaltung des Simulationsmodus
  - \* Anzeige des Logfiles
  - \* Anzeige der Suhosin-Konfiguration, welche bearbeitet werden kann

# Suhosin - Backendmodul

# Suhosin - Backendmodul

# Sicherheitstests: OWASP-Top Ten Risks



# Sicherheitstests: OWASP-Top Ten Risks

# Sicherheitstests: OWASP-Top Ten Risks

# Livedemo

- \* Giessen Aegis
- \* Suhosin

# Fazit

- \* Aktueller Stand:
  - \* Einsatzbereit
  - \* Momentan auf einem Testserver eingebunden
    - \* <http://www-test.mni.fh-giessen.de/administrator/index.php>
    - \* <http://www-test.mni.fh-giessen.de/>
    - \* Aufrufbar nur aus dem FH-Netz (alternativ über [VPN](#))
  - \* SVN-Repository
    - \* Momentan: <http://tracking.mni.fh-giessen.de/svn/joomla/>
    - \* Bald: <http://joomlancode.org/>

# Fazit

- \* Die Grafiken zeigen, dass Joomla! schon gegen die meisten OWASP Risks abgesichert ist, allerdings werden Angriffe weder geloggt, noch werden Gegenmaßnahmen unternommen. Unsere entwickelten Features runden das System soweit ab, dass der Seitenbetreiber eine bessere Übersicht über den Sicherheitsstatus seiner Webseite bekommt.

Vielen Dank für ihre Aufmerksamkeit

ENDE